UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of
3480 2nd Avenue, Los Angeles, CA 90018

Case No. 2:23-MJ-6198

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-1

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 841(a)(1)	Possession with Intent to Distribute Controlled Substances and Distribution of Controlled Substances
21 U.S.C. § 846	Conspiracy and Attempt to Distribute Controlled Substances
21 U.S.C. § 843(b)	Unlawful Use of a Communication facility to Facilitate the Distribution of a Controlled Substance

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Wilford Claiborne

Applicant's signature

Wilford Claiborne, US Postal Inspector

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.
Date: _____

Judge's signature

City and state: Los Angeles, CA

Hon. Jean Rosenbluth, U.S. Magistrate Judge

Printed name and title

AUSA: K. Afia Bondero (x2435)

ATTACHMENT A-1

PREMISES TO BE SEARCHED

The SUBJECT PREMISES to be searched is a single-family residence with a detached garage, located at 3480 2nd Avenue Los Angeles, CA 90018. The residence is green in color with white trim around the windows. The front door is brown with glass inserts. The residence has a detached garage. The premises to be searched includes all garages, sheds, and storage areas in close proximity to the SUBJECT PREMISES, and any vehicles parked in the garage, on the premises, on the driveway of SUBJECT PREMISES.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances), 846 (conspiracy and attempt to distribute controlled substances), and 843(b) (unlawful use of a communication facility, including the mails, to facilitate the distribution of a controlled substance) (the "Subject Offenses"), namely:

a. Any controlled substance, controlled substance analogue, or listed chemical;

b. Items and paraphernalia for the manufacturing, distributing, packaging, sale, or weighing of controlled substances, including scales and other weighing devices, plastic baggies, food saver sealing devices, heat sealing devices, balloons, packaging materials, containers, and money counters;

c. Items used in the packaging of currency for consolidation and transportation, such as money-counting machines, money wrappers, carbon paper, rubber bands, duct tape or wrapping tape, plastic wrap or shrink wrap, and plastic sealing machines;

d. United States currency over $1,000 or bearer instruments worth over $1,000 (including cashier's checks, traveler's checks, certificates of deposit, stock certificates, and bonds) (including the first $1,000), and data, records, documents, or information (including electronic mail, messages

over applications and social media, and photographs) pertaining to, obtaining, possessing, using, applications for, or transferring money over $1,000, such as bank account records, cryptocurrency records and accounts;

e. Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply of controlled substances, or drug customers, including calendars, address books, telephone or other contact lists, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed, whether contained in hard copy correspondence, notes, emails, text messages, photographs, videos (including items stored on digital devices), or otherwise;

f. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

g. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;

h. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

i. Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs;

j. Contents of any calendar or date book;

k. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

l. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

m. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created,

modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICE(S)

4. In searching digital devices (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar

facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized,

the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

7. During the execution of this search warrant, law enforcement is permitted to: (1) depress Samuel Cohen's thumb- and/or fingers onto the fingerprint sensor of the digital device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of Samuel Cohen's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

8. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not

apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Wilford Claiborne, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of an application for warrants to search the following:

a. 3480 2nd Avenue, Los Angeles, CA 90018 (the "SUBJECT PREMISES"), as described more fully in Attachment A-1; and

b. a 2021 Mazda CX-30, bearing vehicle identification number 3MVDMBCL2MM238683 and California license plate 8WHT369 (the "SUBJECT VEHICLE"), as described more fully in Attachment A-2.

2. The person of SAMUEL ELI COHEN ("COHEN"), as described more fully in Attachment A-3.

3. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of 21 U.S.C. §§ 841(a)(1) (distribution of and possession with intent to distribute controlled substances), 846 (conspiracy and attempt to distribute controlled substances), and 843(b) (unlawful use of a communication facility, including the mail, to facilitate the distribution of a controlled substance) (the "Subject Offenses"), as described more fully in Attachment B. Attachments A-1, A-2, A-3, and B are incorporated herein by reference.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and

information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrants, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND OF AFFIANT

5. I am a United States Postal Inspector with the United States Postal Inspection Service ("USPIS"), Los Angeles Division, and have been so employed since August 2013. From August 2013 until November 2017, I was assigned to the Los Angeles Mail Theft Team. I am currently assigned to the Prohibited Mailing and Illegal Narcotics Team. I have completed a twelve-week Postal Inspector Basic Training course, which included training in the investigation of drug distribution via the United States mail. I have conducted numerous investigations into drug distribution and money laundering involving the United States mail. I am familiar with the ways in which drug distributors use the mail system to transport drugs and drug proceeds.

III. SUMMARY OF PROBABLE CAUSE

6. On or about June 5, 2023, a USPS parcel was mailed from Pensacola, Florida to "Samuel Eli Cohen PO BOX 24935 Los Angeles CA 90024-0935." A search of the parcel was conducted

pursuant to a federal search warrant. The parcel contained multiple types of pills, including 475 grams of pills which field tested positive for fentanyl.

7. The addressee, "Samuel Eli Cohen" (herein referred to as "COHEN"), was found to be a real person in control of the PO Box the parcel was addressed to as well as another mailbox located in Sherman Oaks, California.

8. Additional investigation revealed COHEN shipped three parcels addressed to the United Kingdom that contained approximately 3,677 grams of marijuana. One of the three parcels was tracked utilizing an I.P. Address for which the subscriber address is the SUBJECT PREMISES. Additionally, the SUBEJCT VEHICLE, which COHEN has been observed driving to pick up and drop off parcels, has also been seen at the SUBJECT PREMISES, along with COHEN.

IV. STATEMENT OF PROBABLE CAUSE

A. COHEN Receives and Sends Packages Containing Controlled Substances

9. On or about June 5, 2023, USPS parcel EI303732175US ("2175 Drug Parcel") was mailed from Pensacola, Florida to "Samuel Eli Cohen PO BOX 24935 Los Angeles CA 90024-0935." On or about June 21, 2023, the Honorable Brianna Fuller Mircheff issued a search warrant authorizing a search of the 2175 Parcel. See 2:23-MJ-03111. I learned from the Postal Inspector who conducted the search of the 2175 Drug Parcel that it contained multiple types of pills, including 475 grams of pills that field

tested positive for fentanyl. I reviewed postal business records for PO BOX 24935 and learned that "Samuel Eli Cohen" ("COHEN") was the registered owner.

10. While reviewing surveillance video from the Village Post Office in Westwood, California, where PO BOX 24935 is located, I observed COHEN[1] ship three USPS Parcels identified by tracking numbers LZ263321625US ("the 1625 Drug Parcel"), LZ263322838US, and LZ238759286US on September 1, 2023. The time stamps from the surveillance video of COHEN dropping the three parcels at the counter are consistent with the postal business records that show the time of the initial scans for the three packages. On September 8, 2023, the Honorable Maria A. Audero issued a search warrant authorizing the search of the three parcels. See 2:23-MJ-04627. A few days later, I opened the three parcels, which contained a total of approximately 3,677 grams of marijuana based on training and experience as well as smell and appearance.

B. COHEN Lives at the SUBJECT PREMISES

11. Soon thereafter, I reviewed postal business records and learned that on September 11, 2023, a user utilizing the IP address 172.112.85.59 (the "IP ADDRESS") tracked the 1625 Drug Parcel. From a federal subpoena return, I learned that the IP

[1] I was able to identify COHEN as the individual who shipped the parcels by comparing his California DMV photo to the individual in the video.

ADDRESS is registered to 3480 2nd Ave, Los Angeles, California 90018 (the "SUBJECT PREMISES").

12. Postal business records also showed that the IP ADDRESS tracked a parcel originating from Prospect, Kentucky. The parcel was identified by USPS tracking number 950550657331325485961 6 (the "9616 Parcel"). On September 14, 2023, I conducted surveillance at the "Federal Mailbox," a commercial mail receiving agency in Sherman Oaks, California, where postal business records had revealed the 9616 Parcel was en route to COHEN at a mailbox located within the business. While surveilling the Federal Mailbox, I saw COHEN pick up a USPS parcel and place it into a Mazda CX-30, identified by California license plate number 8WHT369 (the "SUBJECT VEHICLE").

13. Utilizing Vigilant LEARN, a database which stores photographs taken of vehicles, I later saw a photograph of the SUBJECT VEHICLE parked in front of the SUBJECT PREMISES that was taken on September 6, 2023.

14. I also reviewed postal business records that showed that in early September 2023, COHEN applied for and was accepted as a mailbox renter at the Federal Mailbox. On the application, COHEN signed his name stating, amongst other things, his telephone number was 415-497-8514 (herein referred to as "COHEN's PHONE").

15. On November 16, 2023, I applied for and received a court order to receive cell-site information, commonly referred to as a ping, for COHEN's PHONE. I started receiving GPS data for COHEN's PHONE on or about November 17, 2023. The GPS data I

received included latitude and longitude coordinates of COHEN's PHONE with an average accuracy of approximately 300 meters.

16. Based on the ping data from COHEN's PHONE, I believe COHEN has been at the SUBJECT PREMISES daily, except the Thanksgiving holiday. Specifically, since obtaining the ping data and through December 5, 2023, I have observed ping data from COHEN's telephone reflecting its presence at or near the SUBJECT PREMISES consistently at nighttime hours. On or about November 28, 2023, I conducted surveillance. COHEN's PHONE ping data placed it at or near the SUBJECT PREMISES. At approximately 9:00 A.M., I saw the SUBJECT VEHICLE parked in the driveway of the SUBJECT PREMISES. At approximately 10:13 A.M., I saw COHEN exit from within the SUBJECT PREMISES to walk a dog.

17. Based on the above, I believe COHEN resides at the SUBJECT PREMISES and is the primary driver of the SUBJECT VEHICLE. I believe COHEN utilized a digital device located within the SUBJECT PREMISES to track the 1625 Drug Parcel. I believe evidence of that activity as well as other narcotic related events are located within the SUBJECT PREMISES. Additionally, I know COHEN utilizes the SUBJECT VEHCILE to pick up and drop off parcels which I believe are also related to COHEN distributing narcotics. From my training and experience I know that people who distribute narcotics through the mail often keep USPS receipts, USPS boxes, and ledgers in their residence and/or vehicle(s) in connection with their drug distribution activity.

VI. TRAINING AND EXPERIENCE ON DRUG OFFENSES

18. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package, and deliver the drugs and launder the drug proceeds. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities in order to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds.

b. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. The aforementioned records are often maintained where drug traffickers have ready access to them, such as on their cell phones and other digital devices, and in their residences.

c. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of the drugs between the seller and the buyer, the negotiation of price, and discussion of whether participants will bring weapons to a deal. In addition, it is common for people engaged in drug trafficking to

have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

d. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices and in their residence. Drug traffickers often keep records of meetings with associates, customers, and suppliers on their digital devices and in their residence, including in the form of calendar entries and location data.

e. Drug traffickers often use vehicles to transport their narcotics and may keep stashes of narcotics in their vehicles in the event of an unexpected opportunity to sell narcotics arises.

f. Drug traffickers often maintain on hand large amounts of United States currency in order to maintain and finance their ongoing drug trafficking businesses, which operate on a cash basis. Such currency is often stored in their residences and vehicles.

g. Drug traffickers often keep drugs in places where they have ready access and control, such as at their residence or in safes. They also often keep other items related to their drug trafficking activities at their residence, such as digital scales, packaging materials, and proceeds of drug trafficking. These items are often small enough to be easily hidden and thus may be kept at a drug trafficker's residence even if the drug

trafficker lives with others who may be unaware of his criminal activity.

h. It is common for drug traffickers to own multiple phones of varying sophistication and cost as a method to diversify communications between various customers and suppliers. These phones range from sophisticated smart phones using digital communications applications such as Blackberry Messenger, WhatsApp, and the like, to cheap, simple, and often prepaid flip phones, known colloquially as "drop phones," for actual voice communications.

19. Drugs are frequently transported from Los Angeles through the United States Mail, and the proceeds from drug sales are frequently returned to Los Angeles through the mail. These proceeds are generally in the form of cash, money orders, bank checks, or similar monetary instruments in an amount over $1,000.00.

20. I know that it is common for people who use a residence to store drugs they ship through the mail to also use that same residence as the address where they receive packages containing the proceeds from their drug sales.

21. I know that people who distribute narcotics through the mail often keep USPS receipts, USPS boxes, and ledgers in their residence and /or vehicles in connection with their drug distribution activity.

V. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[2]

22. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents,

[2] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

23. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

24. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a

device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress Samuel COHEN's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of Samuel COHEN's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

25. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VI. CONCLUSION

26. For all the reasons above, there is probable cause to believe that the SUBJECT PREMISES, as described in Attachment A-1, the SUBJECT VEHICLE, as described in Attachment A-2, and the person, as described in Attachment A-3, contain evidence, fruits, and instrumentalities of violations of 21 U.S.C.

§§ 841(a)(1) (distribution and possession with intent to distribute a controlled substance), 846 (conspiracy) and 843(b) (unlawful use of a communication facility, including the mails, to facilitate the distribution of a controlled substance), as described in Attachment B.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this ____ day of December 2023.

_____
UNITED STATES MAGISTRATE JUDGE